UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,952	09/03/2004	Alexander Shipp	117-510	1457

23117 7590 10/10/2007

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
10/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,952	SHIPP, ALEXANDER	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/1/05, 7/8/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 are pending.

Claim Objections

2. Claim 1 is objected to because of the following informalities: the preamble appears to be grammatical incorrect. Examiner suggests a correction to read "a system for scanning a computer file containing source code of a computer program in a given computer language for malware comprising." Appropriate correction is required.

3. Claim 7 is objected to because of the following informalities: the preamble appears to be grammatical incorrect. Examiner suggests a correction to read "a method for scanning a computer file containing source code of a computer program in a given computer language for malware comprising." Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Claims 1-6 are rejected under 35 U.S.C. 101** because the claims are directed towards nonstatutory subject matter. The cited claims are means plus function claims

and thus the specification is examined in order to determine the structural elements of the claims. The specification provides that the system is implemented by means of a software automaton. Thus, the cited claims are an example of functional descriptive material consisting of data structures and programs that impart functionality when employed as executed by a computer component. The functionality of functional descriptive material is realized only when the functional descriptive material is claimed as being embodied on a computer readable medium and is claimed as executed by a computer component. The cited claims provide no tangible computer components that work in conjunction with the functional descriptive material to impart functionality and as a result the claims are not statutory because they fail the practical application requirement of § 101 by failing to provide a useful, concrete, and tangible result (see MPEP 2106).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 3, 7, 9-10 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gryaznov et al US Patent No. 7,210,041 in view of Beetz WO 02/10888.

6. **With regards to claims 1, 7,** Gryaznov teaches a system for scanning a computer file containing source code of a computer program in a given computer language for malware (Gryaznov, column 4 lines 45-60, macro virus checker) comprising means for separating the source code into groups of constituent parts corresponding to different structural parts of the program (Gryaznov, column 5 lines 5-12, separates source code into string constants and source code text), means for processing each part (Gryaznov, column 9 lines 4-5, source code and string constants are processed), means for flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means (Gryaznov, column 5 lines 35-40, report and analysis created in a log file). Gryaznov fails to teach counting the occurrences of characters of a character set to obtain a frequency distribution. However, Beetz teaches counting the number of occurrences of characters of a character set (Beetz, page 8 lines 20-25, counts characters within the range of 0-255) to obtain a frequency distribution of characters (Beetz, page 8 lines 20-33, determines frequency distribution) and means for comparing the character frequency distribution with an expected range of frequency distributions (Beetz, page 9 lines 9-17, compares frequency distribution in order to match expected level for compressed files). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Beetz method of using neural networks which analyze character counts because it offers the advantage of aiding in the detection of viruses that are packed in compressed files (Beetz, page 4 lines 1-10).

7. **With regards to claims 3 and 9**, Gryaznov as modified teaches the flagging means is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each part with an expected frequency distribution (Gryaznov, column 6 line 63 – column 7 line 45, both the string constant and source code segments are searched and the accumulated frequency of matches is collected and matched to a single expected virus definition).

8. **With regards to claims 4, 10**, Gryaznov as modified teaches wherein in operation of the comparing means the range of distribution which it considers as representing an acceptable match for the part is varied depending on the number of characters either in part or the program as a whole with fewer characters corresponding to a wide range (Beetz, page 10 lines 12-30, proportion of each byte value for determining matches is normalized by the file size).

9. **Claims 2 and 8 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Gryaznov et al US Patent No. 7,210,041 and Beetz WO 02/10888 as applied to claim 1 above, and further in view of Weber et al "Toolkit for detecting and analyzing malicious software."

10. **With regards to claims 2 and 8**, Gryaznov as modified teaches the flagging means is operative to flag the file as suspect depending upon frequency distribution of one or more of said parts (Beetz, page 9 lines 9-17, compares frequency distribution in order to match expected level for compressed files), but fails to teach the flagging occurring if there is not a match with an expected range. However, Weber teaches

flagging occurring if there is not a match with an expected range (Weber, Section 3.2, determines if entry point address falls within expected section of file). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Weber's method of comparing because it offers the advantage of providing a broader base of malicious software detection by detecting both malicious behavior contained in program code and structural characteristics of malicious code (Weber, Section 2 Background).

11. **Claims 5 and 11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gryaznov et al US Patent No. 7,210,041 and Beetz WO 02/10888 as applied to claim 1 above, and further in view of Crosbie et al US Patent No. 7,134,141.

12. **With regards to claims 5 and 11**, Gryaznov as modified fails to teach an exception list of files. However, Crosbie teaches means for maintaining an exception list of files which by their contents are to be treated as exceptions (Crosbie, column 24 line 55 – column 25 line 10, list of files are designated to be ignored for security processing), means for identifying a file as being included in the exception list (Crosbie, column 24 line 55 – column 25 line 10, ignore if on the list), and wherein a file is not marked as suspect if it is identified as being on the exception list (Crosbie, column 25 lines 6-11, ignore changes to file and do not cause an alert). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of using an exception list because it offers the advantage of helping

detect the modification of a file that is unauthorized or unexpected thus increasing security (Crosbie, column 25 line 58 – column 26 line 5).

13. **Claim 6 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Gryaznov et al US Patent No. 7,210,041 and Beetz WO 02/10888 as applied to claim 1 above, and further in view of Radatti US PGPub 2003/0120953.

14. **With regards to claim 5**, Gryaznov as modified fails to teach duplicate parts are ignored. However, Radatti teaches duplicate parts are ignored (Radatti, paragraph 0050, all like files are ignored). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Radatti's method of ignoring duplicates because it offers the advantage of increasing efficiency by reducing the demand on systems for indexing and scanning (Radatti, paragraph 0027, 0050).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven